FORTINET

FortiOS™ Handbook - What's New for FortiOS 6.0

VERSION 6.0.2

FORTIOS VERSION 6.0

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING AND CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

July 26, 2018

FortiOS™ Handbook - What's New for FortiOS 6.0.2

01-602-481040-20180726

TABLE OF CONTENTS

Change log

Date	Change description
July 26, 2018	FortiOS 6.0.2 document release. New features added: Azure regional support on page 8 and FortiAP-S bridge mode security profiles on page 13.
June 20, 2018	New section added: GUI change for single sign-on configuration on page 8.
June 5, 2018	FortiOS 6.0.1 document release. Minor updates.
April 30, 2018	Minor updates.
March 29, 2018	FortiOS 6.0 document release.

Fortinet Security Fabric

This section introduces new Security Fabric features in FortiOS 6.0.

Security Fabric automation

User-defined Automations allow you to improve response times to security events by automating the activities between devices in the Security Fabric. You can monitor events from any source in the Security Fabric and set up action responses to any destination. To create an Automation, you can set up a Trigger event and response Actions that cause the Security Fabric to respond in a predetermined way. From the root FortiGate, you can set up event triggers for the following event types: compromised host, event log, reboot, conserve mode, high CPU, license expiry, High Availability (HA) failover, and configuration changes. The workflows have the means to launch the following actions in response: email, FortiExplorer notification, AWS Lambda and webhook. Additional actions are available for compromised hosts, such as: access layer quarantine, quarantine FortiClient via EMS, and IP ban.

FortiOS 6.0.2 adds the ability to test automation stitches using the `diagnose automation test` command.

For more information, see the *Fortinet Security Fabric Handbook*.

Security rating

The Security Rating feature (previously called the Security Fabric Audit) includes new security checks that can help you make improvements to your organization's network, such as enforce password security, apply recommended login attempt thresholds, encourage two factor authentication, and more.

For more information, see the *Fortinet Recommended Security Best Practices* document.

Security rating FortiGuard service

Security Rating is now a subscription service that FortiGuard offers when you purchase a Security Rating license. This service allows you to:

- Dynamically receive updates from FortiGuard.
- Run Security Rating checks for each licensed device in a Security Fabric.
- Run Security Rating checks in the background or on demand.
- Submit rating scores to FortiGuard and receive rating scores from FortiGuard, for ranking customers by percentile.

For more information, see the *Fortinet Security Fabric Handbook*.

Solution and service integration

In FortiOS 6.0, the Security Fabric extends to include more Fortinet products.

Wireless user quarantine

When you create or edit an SSID, you can enable the **Quarantine Host** option to quarantine devices that are connected in Tunnel-mode. The option to quarantine a device is available from the **Topology** and **FortiView** WiFi pages.

When a host is put into the quarantine VLAN, it gets an IP address from the quarantine VLAN DHCP server, and becomes part of the quarantined network.

For more information, see the *FortiWiFi and FortiAP Configuration Guide*.

Fortinet products can join the Security Fabric by serial number

Fortinet products can now easily and securely join the Security Fabric using an authorized device serial number.

To learn how to allow a Fortinet product to join your Security Fabric, see the *Fortinet Security Fabric Handbook*.

FortiMail integration

You can now add a FortiMail stats widget to the FortiGate Dashboard page to show mail detection stats from FortiMail. Other FortiMail integrations include the following:

- A FortiMail section that displays the FortiMail name, IP address, login and password is now available in the Security Fabric Settings page.
- FortiMail is now shown as a node in the topology tree view in the Fabric Settings page and in the Physical Topology and Logical Topology views.
- The topology views now show the number of FortiMail devices in the Security Fabric in the device summary.

For more information, see the *Fortinet Security Fabric Handbook*.

Synchronize the FortiManager IP address among all Security Fabric members

When you add a FortiManager to the root FortiGate of the Security Fabric, its configuration is now automatically synchronized with all devices in the Security Fabric. Central management features are now configured from the Security Fabric Settings page.

For more information, see the *Fortinet Security Fabric Handbook*.

Improve FortiAP and FortiSwitch support in Security Fabric views

The Security Fabric widget on the dashboard and the Security Fabric Settings page now show the FortiAP and FortiSwitch devices in the Security Fabric.

- You can now use new shortcuts to easily authorize any newly discovered devices and manage them.
- Switch stacking is now supported in the Physical and Logical topology views, and Inter-switch Link (ISL-LAG) is now identified by a thicker single line.

For more information, see the *Fortinet Security Fabric Handbook*.

EMS server support in Security Fabric topology

The FortiClient Endpoint Management System (EMS) can be enabled in FortiClient Endpoint profiles. This feature allows you to maintain FortiClient endpoint protection from FortiClient EMS and dynamically push configuration changes from the EMS to FortiClient endpoints. EMS server support is also integrated with Security Fabric Automation.

For more information, see the *Fortinet Security Fabric Handbook*.

Multi-cloud support (Security Fabric connectors)

Security Fabric multi-cloud support adds Security Fabric connectors to the Security Fabric configuration. Security Fabric connectors allow you to integrate Application Centric Infrastructure (ACI), Amazon Web Services (AWS), Microsoft Azure, VMware NSX, and Nuage Virtualized Services Platform configurations into the Security Fabric.

Additionally Cloud init support for Azure is now native to the cloud. FortiGate VM for Azure also supports bootstrapping.

For more information, see the *Fortinet Security Fabric Handbook* and the *Virtual FortiOS Handbook (Private Cloud Administration Guide)*.

Azure regional support

The Azure Security Fabric connector supports connecting to regional Azure public clouds. This change allows organizations in different regions to connect to their regional Azure public cloud if required for compliance or performance reasons.

For more information, see the *Fortinet Security Fabric Handbook* and the *Virtual FortiOS Handbook (Private Cloud Administration Guide)*.

GUI change for single sign-on configuration

In FortiOS 6.0.1, the options to configure single sign-on in the FortiGate GUI are now located in the **Security Fabric > Fabric Connectors** menu.

Manageability

This section introduces new manageability features in FortiOS 6.0.

Asset tagging

You can use the new Asset Tagging system to create tags to separate and categorize network objects, interfaces, and devices. Tags are flexible, easy to configure, and useful for comprehensive monitoring, audit reporting, and more.

For more information, see the *System Administration Handbook*.

FortiSwitch network assisted device detection and destination name resolution

Device detection now extends to managed FortiSwitches since some devices may not be visible to the FortiGate that manages them. Devices that are connected to a FortiSwitch are more visible to the FortiGate that manages them and to the Security Fabric.

FortiSwitch destination name resolution clearly presents destination objects and the aggregation of related IP addresses with domains. It also applies Internet Service Database (ISDB) mapping for destination data.

For more information, see the *Managing Devices Handbook* and the *FortiSwitch Devices Managed by FortiOS 6.0 Handbook*.

Global security profiles

Global Security Profiles can be used by multiple VDOMs instead of creating identical profiles for each VDOM. You can create global security profiles for the following security features:

- Antivirus
- Application control
- Data leak prevention
- Intrusion protection
- Web filtering

For more information, see the *Virtual Domains Handbook*.

Networking

This section introduces new networking features in FortiOS 6.0.

SD-WAN improvements

FortiOS 6.0 introduces the following SD-WAN features:

- Multiple server support for health checks
- Internet service groups
- Bandwidth options in SD-WAN rules
- Custom profiles in SD-WAN rules
- DSCP tagging of forwarded packets in SD-WAN rules

For more information, see the *Networking Handbook*.

Multipath intelligence and performance SLAs

SD-WAN performance Service-Level Agreements (SLAs) incorporate multilayer SLA monitoring of link selection. To help handle emergency load or outages you can select links based on weight and SLA priority and then return to defaults once the network stabilizes. Also, traffic shaping and application intelligence have been added to the SD-WAN configuration, which gives you more control of SD-WAN traffic.

For more information, see the *Networking Handbook*.

Application awareness

You can now use application control and application control group options in SD-WAN rules.

Internet Service support is also increased from a single Internet Service to Internet Service groups.

For more information, see the *Networking Handbook*.

BGP dynamic routing and IPv6 support for SD-WAN

FortiOS 6.0 introduces support for dynamic router for an SD-WAN configuration. You can set up a route map and add a route tag to the route map. Then, you can create an SD-WAN configuration, a health check, and a service for it. When you create the service, you add the configured route tag that you created in the route map to the service.

For more information, see the *Networking Handbook*.

Interface-based traffic shaping

In FortiOS 6.0, you can now enable traffic shaping on an interface. Interface-based traffic shaping allows you to enforce bandwidth limits by traffic type for individual interfaces.

For more information, see the *Traffic Shaping Handbook*.

Cloud-assisted one-click VPN

One-click VPN (OCVPN) is a cloud-based solution that greatly simplifies the provisioning and configuration of IPsec VPN. The administrator enables OCVPN with a single click, adds the required subnets, and then the configuration is complete. The OCVPN updates each FortiGate automatically as devices join and leave the VPN, as subnets are added and removed, when dynamic external IP addresses change (for example, DHCP or PPPoE), and when WAN interface bindings change (as in the case of dual WAN redundancy).

For more information, see the *IPsec VPN Handbook*.

IPv6 enhancements

The following new IPv6 features have been added.

- IPv6 captive portal
- IPv6 FQDN and wildcard firewall addresses
- IPv6 ISIS dynamic routing
- DHCPv6 server prefix delegation
- IPv6 DFD and VRRP

For more information, see the *Firewall Handbook*.

NAT enhancements

The following new NAT features have been added.

- Central source NAT (SNAT) policies now include a comment field
- Port block allocation timeout is configurable
- NAT46 IP pools
- VRRP HA supports firewall virtual IPs (VIPs) and IP pools

For more information, see the *Firewall Handbook*.

EMAC-VLAN support

The media access control (MAC) virtual local area network (VLAN) feature in Linux allows you to configure multiple virtual interfaces with different MAC addresses (and therefore different IP addresses) on a physical interface.

For more information, see the *Networking Handbook*.

Security

This section introduces new security features in FortiOS 6.0.

FortiGuard virus outbreak prevention

FortiGuard virus outbreak prevention is an additional layer of protection that keeps your network safe from newly emerging malware. Quick virus outbreaks can infect a network before signatures can be developed to stop them. Outbreak protection stops these virus outbreaks until signatures become available in FortiGuard.

For more information, see the *Security Profiles Handbook*.

FortiGuard content disarm and reconstruction

Content Disarm and Reconstruction (CDR) removes exploitable content and replaces it with content that's known to be safe. As files are processed through an enabled AntiVirus profile, content that's found to be malicious or unsafe is replaced with content that allows the traffic to continue, but doesn't put the recipient at risk.

Content that can be scanned includes PDF and Microsoft Office files leaving the network on CDR-supported protocols (such as, HTTP web download, SMTP email send, IMAP and POP3 email retrieval—MAPI isn't supported).

This feature works even if FortiSandbox is not configured, but only if you want to discard the original file. If FortiSandbox is configured and it responds that the file is clean, it passes the content unmodified.

For more information, see the *Security Profiles Handbook*.

Application groups for NGFW policies

When a FortiGate operates in NGFW policy mode, you can create application groups when you add NGFW policies. Then, when you add IPv4 or IPv6 policies you can create application groups to simplify policy creation.

For more information, see the *Firewall Handbook*.

Application control rule sequencing

To have more control over application control outcomes, you can control the order that application signatures appear in application control sensors. Signatures for applications that are more sensitive can appear higher in the list so they get matched first.

For more information, see the *Security Profiles Handbook*.

Threat Feeds (external dynamic block lists)

This feature introduces the ability to dynamically import external block lists from an HTTP server. You can use the block lists to enforce special security requirements that your organization has. This can include long term policies to always block access to some websites or short time requirements to block access to known compromised locations. Since the lists are dynamically imported any changes made to the list are instantly imported by FortiOS. Dynamic block lists can be added to:

- Web Filter profiles and SSL inspection exemptions.
- DNS Filter profiles and "Source/Destination" addresses in proxy policies.

In each profile, the administrator can configure multiple external block lists.

For more information, see the *Security Profiles Handbook*.

FortiAP-S bridge mode security profiles

If you have enabled bridge mode for a managed FortiAP-S, you can add a UTM profile to the wireless controller configuration that allows you to apply the following security profile features to all traffic accepted by the managed FortiAP-S:

- AntiVirus (including Botnet protection),
- IPS,
- Application control, and
- Web Filtering.

For more information, see the *FortiWiFi and FortiAP Configuration Guide*.